REMARKS

Claims 1-13 and 15 were pending in the patent application. By this amendment, Claims 12 and 15 are canceled and amendments are introduced for Claims 1, 6, 9, 11, and 13. The Examiner has stated that the drawings are objected to; has rejected Claim 6 under 35 USC 112 as indefinite; has rejected Claims 12-13 and 15 under 35 USC 101 as nonstatutory subject matter; and, has rejected Claims 1-15 under 35 USC 102 as anticipated by the Schaefer-Lorinser patent. Applicants submit herewith new drawings and claims' amendment to address the objections and 112 rejections. With regard to the 101 rejections, the relevant claims, Claims 12 and 15, have been canceled and Claim 13 has been amended to depend from Claim 1. For the reasons set forth below, Applicants believe that the remaining claims, as amended, are patentable over the Schaefer-Lorinser patent.

The present invention teaches and claims a signature device, such as a chipcard, which includes a signature program and additional signature certificate information for providing an expanded electronic signature to sign a document (page 6, lines 16-22). The signature device

GE998-005   -8-

executes the signature program and does not require that an external authenticating entity generate the digital signature when the user is attempting to digitally sign a document ("the external and internal information together with the hash are merged on the chipcard 101", from page 13, line 14; "merger is effected by the chipcard program", from page 13, line 18; and, "[t]his encryption takes place on the chipcard", from page 14, lines 11-12). The digital signature includes an identifier of the signature device as well as at least one identifying characteristic indicating the hardware and software environment used in generating the electronic signature (see: page 3, lines 1-3; page 4, lines 1-4; page 13, lines 4-7; and page 15, lines 6-9) as well as a document extract value identifying the document which is being signed (see: page 12, lines 19-20; and page 14, lines 23-24). All of the independent claims, Claims 1, 9, 11, and 12 as amended, expressly recite that the signature device stores the signature program which is to be executed as well the necessary additional information so that it can perform digital signing of a document, and that the digital signing incorporates an identifier of the signature device as well as at least one characteristic indicating the hardware and software environment used in generating the signature, as

GE998-005   -9-

well as a document extract value for the document to be signed.

The Schaefer-Lorinser patent is directed to a system for secured reading and processing of data on intelligent data carriers, even when the terminal which is reading and processing the data is not connected to a server for authentication of the data carrier. Under the Schaefer-Lorinser system and method, the data carrier (i.e., the chipcard) and the terminal exchange cryptograms for authentication of the data carrier. Data used for generating a cryptogram at the data carrier is encoded at the data carrier when it is first issued (see: Col. 3, lines 51-55). Similarly, data used for generating cryptograms at the terminal is permanently stored at the terminal (see: Col. 4, lines 6-8), so that connection to a server is not required for authentication. As taught by Schaefer-Lorinser at Col. 3, lines 52-56, the data carrier/chipcard has a certificate "representing an electronic signature". When the data carrier generates a so-called "acknowledgment crytogram" (Col. 4, lines 61-64) that is the electronic signature, e_3, (see, Fig. 2) the data carrier applies a signature function S_{card} (defined at Col. 3, lines 65) on a data set comprising the ID number of the data carrier, a

GE998-005   -10-

posting data record, D_B, (see: Col. 4, lines 54-55) and a random number, R_3, which has been generated by the terminal (se: Col. 4, lines 47-48).

Applicants respectfully assert that the Schaefer-Lorinser patent does not teach or suggest the invention as claimed. While Schaefer-Lorinser does receive R_3 as input information to the signature device, Applicants believe that the Schaefer-Lorinser does not teach or suggest the steps and means for performing the steps of executing the signature program including the claimed creating and encrypting. The present invention first creates a signature data set which comprises the received input information, an identifier to identify the signature device, at least one identifying characteristic of the hardware and software environment used for generating said digital signature, and a document extract value.

Schaefer-Lorinser does not teach or suggest the existence or use of an identifying characteristic of the hardware and software environment used for generating the digital signature. Such is clearly taught by the present Specification, for example on page 13, lines 1-12, to include, in addition to an identifier, a signature counter value, an indication of the encryption method used, or an

GE998-005   -11-

identifier of the program such as a license number or program serial number, and is now expressly claimed. Furthermore, the Schaefer-Lorinser use of a "posting data record" is not the same as or suggestive of a document extract value of a document for signing, as is taught and claimed for the present invention. Schaefer-Lorinser's posting data record records the currency and amount of the debit and the posting number and time. Such information is not a document extract value.

It is well established under U. S. Patent Law that, for a reference to anticipate claim language under 35 USC 102, that reference must teach each and every claim feature. Since the Schaefer-Lorinser patent does not teach the signature device and method as claimed, including means and steps for a signature device, having a signature program and certificate, to generate a digital signature which identifies the signature device and at least one characteristic of the environment used to generate the signature, and uses a document extract value for the document to be signed, it cannot be maintained that the Schaefer-Lorinser patent anticipates the invention as set forth in the independent claims, Claims 1, 9 and 11. Moreover, a reference which does not anticipate the language

GE998-005   -12-

of an independent claim cannot be said to anticipate the language of claims which depend therefrom and add further limitations thereto.   Accordingly, Applicants respectfully assert that the Schaefer-Lorinser patent does not anticipate the language of Claims 2-8, 10, and 13.

With specific reference to the language of the dependent claims, Applicants note that the teachings cited against Claim 2, from Col. 4, lines 17-23, provide no mention of a signature counter.   Clearly, therefore, the cited teachings do not anticipate the language of Claim 2, and of Claim 3 which depends therefrom.

Applicants note that the teachings from Col. 4, lines 23-65, cited against Claim 3, also do not mention a counter as an attribute of a signature key.   The mention of a chipcard posting sequence number (i.e., debit record) is not the same as having a signature counter as an attribute of a signature key.   Moreover, the Schaefer-Lorinser posting sequence number is noted as part of its D_B value and not as an attribute of a signature key.

With regard to Claim 4, the Examiner has cited the passage from Col. 4, lines 36-51.   The actions described therein are exclusively performed at the terminal, which

GE998-005   -13-

clearly cannot anticipate a receiving step at the signature device.

With regard to Claim 5, the cited passage from Col. 3, lines 23-32 discusses that for "electronic purse" applications, a terminal is not connected to a server. The passage does not, however, make any mention of a terminal procuring information about the hardware and software environment used to create a digital signature.

With regard to Claim 6, and Claims 7-8 which depend therefrom, the cited passage from Col. 4, lines 23-45 does not make any mention of a holder of a signature key. Clearly, therefore, the cited passage does not anticipate the invention as claimed.

Claim 13 recites that additional information uniquely identifies the digital signature in relation to every other digital signature generated with the same signature key. However, the cited passage from Col. 4, lines 45-51 makes no mention of any other digital signatures, let alone of including an indication thereof in a signature data set to be encrypted.

GE998-005   -14-

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

E. Hamann, et al

By: _____
Anne Vachon Dougherty
Registration No. 30,874
Tel. (914) 962-5910

GE998-005   -15-